SDWSCS (IMPLEMENTING CISCO SD-WAN SECURITY AND CLOUD SOLUTIONS) 1.0

Objetivo

Upon completing this course, students will be able to meet these objectives: â□¢ Describe Cisco SD-WAN security functions and deployment options; â□¢ Understand how to deploy on-premises threat prevention; â□¢ Describe content filtering options; â□¢ Implement secure Direct Internet Access (DIA); â□¢ Explain and implement service chaining; â□¢ Explore Secure Access Service Edge (SASE) and identify use cases; â□¢ Describe Umbrella Secure Internet Gateway (SIG) and deployment options; â□¢ Implement Cisco Umbrella SIG and DNS policies; â□¢ Explore and implement Cloud Access Security Broker (CASB) and identify use cases (including Microsoft 365); â□¢ Discover how to use Cisco ThousandEyes to monitor cloud services; â□¢ Configure Cisco ThousandEyes to monitor Microsoft 365 applications; â□¢ Examine how to protect and optimize access to the software as a service (SaaS) application with Cisco SD-WAN Cloud OnRamp; â□¢ Discover and deploy Cloud OnRamp for multi-cloud, including interconnect and collocation use cases; â□¢ Examine Cisco SD-WAN monitoring capabilities and features with vManage and vAnalytics.

PÃºblico Alvo

â□¢ Network Engineers; â□¢ Network Security Engineers; â□¢ Network Architects.

PrÃ©-Requisitos

The knowledge and skills that students are expected to have before attending this course are: â□¢ Basic understanding of enterprise routing; â□¢ Basic understanding of WAN networking; â□¢ Basic understanding of Cisco SD-WAN; â□¢ Basic understanding of Public Cloud services. Here are recommended Cisco learning offerings that may help students meet these prerequisites: â□¢ Implementing and Administering Cisco Solutions (CCNA) v1.0; â□¢ Implementing Cisco SD-WAN Solutions (ENSDWI) v2.0; â□¢ Cisco SD-WAN Operation and Deployment (SDWFND) v1.0.

Carga HorÃ¡ria

24 horas (3 dias).

ConteÃºdo ProgramÃ¡tico

Course Introduction
Overview
Course Goal and Objectives
Course Flow
Your Training Curriculum
Learner Introductions

Introducing Cisco SD-WAN Security
SD-WAN Security Functions and deployment options This Cisco SD-WAN Security Overview
Cisco SD-WAN Platform
Cisco SD-WAN Security Types

Deploying On-Premises Threat Prevention
Cisco SD-WAN on-box and integrated threat prevention security services
Cisco SD-WAN Integrated Security Overview
Deploying Application Aware Firewall
Deploying Intrusion Prevention

Discovery 1: Configure Threat Prevention
Objectives: Deploy and verify security policies by using Cisco vManage
Task 1: Prepare the Lab Environment
Task 2: Verify Lab Environment
Task 3: Secure Internet Access with the Application-Aware Enterprise Firewall
Task 4: Secure Internal Traffic with Application-Aware Enterprise Firewall
Task 5: Secure Internal Traffic with Intrusion Prevention

Examining Content Filtering
SD-WAN on-box and integrated content filtering security services
Cisco SD-WAN Content Filtering
Implementing Web Security Functionalities
Implementing Cisco SD-WAN SSL and TLS Proxy

Discovery 2: Implement Web Security
Objectives: Design, deploy, and verify SSL and TLS Decryption and Cisco URL Filtering Security policy by using Cisco vManage Device and Security templates
Task 1: Prepare the Lab Environment
Task 2: Verify Lab Environment
Task 3: Configure Cisco vManage CA
Task 4: Create Cisco URL Filtering and TLS Proxy Policies
Task 5: Deploy Cisco URL Filtering and TLS Proxy Policies

Implementing File Security
Secure Direct Internet Access
Implementing Unified Security Policies

Discovery 3: Deploy DIA Security with Unified Security Policy
Objectives: Design, deploy, and verify a unified security policy to secure DIA at remote branch sites
Task 1: Prepare the Lab Environment
Task 2: Verify Lab Environment
Task 3: Create Advanced Inspection Profiles
Task 4: Design and Deploy a Unified Security Policy

Exploring Cisco SD-WAN Dedicated Security Options
Integration of Cisco SD-WAN with dedicated security SNGFW and IPS with service chaining
Integrating Cisco SD-WAN with Dedicated Security

Service Chaining Deep Dive
Deploying Service Chaining
Troubleshooting Service Chaining
Deploying TrustSec on Cisco SD-WAN

Discovery 4: Deploy Service Chaining
Objectives: Design, deploy, and verify service chaining policies to force specific traffic (Cisco FTD)
Task 1: Prepare the Lab Environment
Task 2: Verify Lab Environment
Task 3: Advertise Network Service into SD-WAN Fabric
Task 4: Deploy Service Chaining with Control Policy
Task 5: Deploy Service Chaining with Data Policy

Examining Cisco SASE
Introduce the Cisco SASE solution
Differences between SASE and SD-WAN
Introducing Cisco SASE Architecture
Cisco Security Vision—Cisco SASE
Implementing Cisco SASE

Exploring Cisco Umbrella SIG
Using Cisco Umbrella SIG as DNS Security, CDFW, IPS, and interaction with Cisco SD-WAN
SIG Overview
Integrating SIG and Cisco SD-WAN
Umbrella DNS Deep Dive
Cisco Umbrella CDFW and IPS
Umbrella Secure Web Gateway

Discovery 5: Configure Cisco Umbrella DNS Policies
Objectives: Integrate the Cisco SD-WAN network with the Cisco Umbrella Secure DNS service
Task 1: Prepare the Lab Environment
Task 2: Verify Lab Environment
Task 3: Integrate Cisco SD-WAN Site with Cisco Umbrella
Task 4: Configure DNS Policy in Cisco Umbrella
Task 5: Test Cisco Umbrella DNS Policy

Discovery 6: Deploy Cisco Umbrella Secure Internet Gateway
Objectives: Explore the Cisco Umbrella SIG and integrate with the Cisco SD-WAN and deployment with the Cisco Umbrella SIG and deploy policies to route internet-bound traffic
Task 1: Prepare the Lab Environment
Task 2: Verify Lab Environment
Task 3: Integrate Cisco SD-WAN Branch Site with Cisco Umbrella SIG
Task 4: Route Traffic to Cisco Umbrella SIG
Task 5: Configure Web Policy in Cisco Umbrella and Verify Policy Enforcement

Securing Cloud Applications with Cisco Umbrella SIG
Explore the Cisco Umbrella SIG use case to secure cloud application access
Discover and control access to cloud delivered applications

Cloud Application Security Overview
Implementing Cisco Umbrella CASB

Discovery 7: Implement CASB Security
Objectives: Design, deploy and verify Umbrella Security Policy and Control and protect customer cloud services using Cisco Umbrella as Cisco SD-WAN CASB
Task 1: Prepare the Lab Environment
Task 2: Verify Lab Environment
Task 3: Integrate Cisco SD-WAN Branch Site with Cisco Umbrella SIG
Task 4: Configure Cisco Umbrella Tenant Control Security Policy
Task 5: Control Access to SaaS Application (Microsoft 365) using Cisco Umbrella Web Security Policy
Task 6: Verify Applied Cisco Umbrella Web Security Policy Rules